(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3926377 A1**

(51) Int. Cl. 5:
F02D 41/22
F 02 D 41/26
F 02 D 41/38

(21) Aktenzeichen: P 39 26 377.0
(22) Anmeldetag: 4. 8. 89
(43) Offenlegungstag: 7. 2. 91

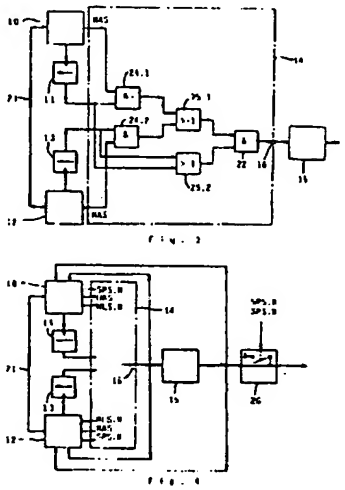
DE 3926377 A1

(71) Anmelder:
Robert Bosch GmbH, 7000 Stuttgart, DE

(72) Erfinder:
Locher, Johannes, Ing.(grad.), 7000 Stuttgart, DE; Graf, Herbert, Dipl.-Ing. (FH), 7257 Ditzingen, DE; Fahrbach, Wilhelm, Dipl.-Ing. (FH), 7102 Weinsberg, DE; Daniilidis, Georgios, Dipl.-Ing. (FH), 7000 Stuttgart, DE; Zimmermann, Werner, Dr.-Ing., 7016 Gerlingen, DE

(54) Elektronisches Steuergerät für eine Brennkraftmaschine

Ein elektronisches Steuergerät für eine Brennkraftmaschine verfügt unter anderem über einen Hauptrechner (10) mit zugeordnetem ersten Watchdog (11), einen Nebenrechner (12) mit zugeordnetem zweiten Watchdog (13) und über Mittel zur Signalausgabe (14). Das Steuergerät gibt über einen Steuerausgang (16) ein Ausgangssignal an ein gesteuertes Bauteil (15). Einer der Pegel des Ausgangssignals stellt ein Sicherheitspotential dar. Dieses Sicherheitspotential bewirkt, daß das Bauteil (15) einen Sicherheits-Betriebszustand einnimmt.
Der Aufbau des Steuergeräts gewährleistet, daß die Ausgangssignale für die Steuerung immer nur dann ausgegeben werden, wenn die Wahrscheinlichkeit sehr hoch ist, daß diese Werte ordnungsgemäß berechnet worden sind.



DE 3926377 A1

Beschreibung

Die Erfindung betrifft ein elektronisches Steuergerät mit mindestens einem Ausgang zum Ausgeben von digitalen Steuersignalen an mindestens ein steuerbares Bauteil einer Brennkraftmaschine, z. B. an ein Stellwerk für eine Dieseleinspritzpumpe.

Stand der Technik

Elektronische Steuergeräte für eine Brennkraftmaschine weisen häufig zwei Rechner auf, die im folgenden als Hauptrechner und als Nebenrechner bezeichnet werden. Der Nebenrechner überwacht u.a. den Hauptrechner und übt bei Ausfall desselben Notfunktionen aus. Bei verschiedenen Steuergeräten hat der Nebenrechner nur diese Funktionen. Bei anderen Steuergeräten unterstützt der Nebenrechner den Hauptrechner auch bei ordnungsgemäßem Betrieb maßgeblich bei den Steuerungsaufgaben. Jeder der beiden Rechner kann Notfunktionen ausüben, wenn der andere Rechner ausfällt.

Der Nebenrechner überwacht den Hauptrechner mit Hilfe von Daten, die über eine Datenleitung zwischen den beiden Rechnern ausgetauscht werden. Darüber hinaus werden beide Rechner durch einen Watchdog überwacht, der von beiden Rechnern getriggert wird. Solange mindestens einer der Rechner das Triggersignal für den Watchdog ausgibt, liefert dieser ein Durchlaßsignal an ein Sperrglied vor dem Steuerausgang. Sobald am Sperrglied das Signal vom Watchdog nicht mehr ansteht, gibt das Sperrglied den Pegel logisch "0" aus. Dieser Pegel entspricht einem Sicherheitspotential, das dafür sorgt, daß das angesteuerte Brennkraftmaschinen-Bauteil in eine Stellung überführt wird, die dafür sorgt, daß der Ausfall des Steuergeräts nicht zu einer Gefährdung von Personen führt, die sich in dem Fahrzeug mit der überwachten Brennkraftmaschine befinden.

Sobald der Nebenrechner feststellt, daß der Hauptrechner ausgefallen ist, gibt er ein Übernahmesignal aus, das einem Signalausgabemittel anzeigt, daß nun die Ausgangssignale vom Nebenrechner auf den Steuerausgang gegeben werden sollen. Problematisch ist, daß der Nebenrechner das Übernahmesignal auch aufgrund einer Fehlfunktion ausgeben kann. Dann wird das Signal vom Hauptrechner vom Steuerausgang weggenommen und auf das Signal vom Nebenrechner umgeschaltet, obwohl dieser fehlerhaft arbeitet.

Es besteht grundsätzlich das Problem, ein elektronisches Steuergerät mit einem Hauptrechner und einem Nebenrechner anzugeben, das so ausgestaltet ist, daß die Überwachung dahingehend, daß nicht unerwünschte Ausgangssignale auftreten, so zuverlässig ist wie möglich.

Darstellung der Erfindung

Die Erfindung betrifft verschiedene Ausgestaltungen elektronischer Steuergeräte mit besonders hoher Zuverlässigkeit. Alle erfindungsgemäßen Steuergeräte gehören zur bekannten Gruppe von Steuergeräten mit den folgenden Merkmalen:

- einem Hauptrechner,
- einem Nebenrechner, der den Hauptrechner überwacht und bei Ausfall desselben Notfunktionen ausübt,

- einer Watchdog-Schaltung für die Rechner, und
- einem Signalausgabemittel zum Ausgeben von Signalen mit zwei Pegeln auf jeden Steuerausgang, wobei einer der Pegel ein Sicherheitspotential aufweist, das bei dauerndem Vorhandensein für einen Sicherheits-Betriebszustand der Brennkraftmaschine sorgt.

Von besonderem Vorteil ist es, wenn die Watchdog-Schaltung über zwei Watchdogs verfügt, nämlich einen ersten Watchdog zum Überwachen der Funktion des Hauptrechners und einen zweiten Watchdog zum Überwachen der Funktion des Nebenrechners.

Beim Steuergerät gemäß Anspruch 1 ist das Signalausgabemittel so ausgebildet, daß es

- die Ausgangssignale vom Nebenrechner an den jeweils zugehörigen Steuerausgang gibt, wenn mindestens die Bedingungen erfüllt sind, daß der Nebenrechner ein Übernahmesignal ausgibt und gleichzeitig der zweite Watchdog meldet, daß der Nebenrechner ordnungsgemäß arbeitet,
- aber grundsätzlich das Sicherheitspotential an jeden Steuerausgang gibt, wenn beide Watchdogs den Ausfall der überwachten Rechner melden.

Durch diese Maßnahmen ist gewährleistet, daß das Signal vom Nebenrechner nur dann auf den mindestens einen Steuerausgang gegeben wird, wenn die Wahrscheinlichkeit sehr hoch ist, daß der Nebenrechner ordnungsgemäß arbeitet, was dadurch angezeigt wird, daß am Ausgang des zweiten Watchdogs ein entsprechendes Signal ansteht.

Das Steuergerät gemäß Anspruch 1 gibt die Ausgangssignale vom Nebenrechner auch dann an die Steuerausgänge, wenn nur der Nebenrechner fehlerhaften Betrieb des Hauptrechners anzeigt, der erste Watchdog aber unverändert ordnungsgemäßen Betrieb des Hauptrechners meldet. Beim Steuergerät gemäß Anspruch 2 ist das Signalausgabemittel so weitergebildet, daß es auch im eben genannten Fall das Sicherheitspotential an jeden Steuerausgang gibt.

Eine ähnliche Funktion wie das Steuergerät gemäß Anspruch 2 weist das Steuergerät gemäß Anspruch 3 auf. Es bietet ebenfalls eine Lösung für den Fall an, daß beide Watchdogs ordnungsgemäßen Betrieb der zugehörigen Rechner melden, der Nebenrechner jedoch auf fehlerhaften Betrieb des Hauptrechners entscheidet. Beim Steuergerät gemäß Anspruch 3 wird in diesem Fall nicht grundsätzlich das Sicherheitspotential an die Steuerausgänge gegeben wie beim Gerät gemäß Anspruch 2, sondern es ist nach wie vor möglich, Ausgangssignale unterschiedlicher Pegel auf Steuerausgänge zu legen, was aber immer nur dann geschieht, wenn die Ausgangssignale der beiden Rechner für den Steuerausgang übereinstimmen.

Wie aus dem Vorstehenden ersichtlich, ist für die Gesamtfunktion des Steuergeräts die Funktion der Watchdog-Schaltung entscheidend. Das Steuergerät gemäß Anspruch 4 ist in vorteilhafter Weise so ausgestaltet, daß die Rechner Überwachungssignale an die Watchdog-Schaltung geben und sie die Ausgangssignale der Watchdog-Schaltung nach dem Ausgeben der Überwachungssignale überprüfen. Das Signalausgabemittel legt das Sicherheitspotential auf die Steuerausgänge, wenn die Überprüfung ergibt, daß die Watchdog-Schaltung nicht ordnungsgemäß arbeitet. Die Watchdog-Schaltung kann aus einem gemeinsamen Watchdog für beide

Rechner, wie beim Stand der Technik, bestehen, oder es kann eine Watchdog-Schaltung mit zwei einzelnen Watchdogs sein, wie bei den Steuergeräten gemäß den Ansprüchen 1 – 3.

Selbst wenn Fehlfunktionen der Rechner ordnungsgemäß festgestellt werden, besteht immer noch die Gefahr, daß fehlerhafte Ausgangssignale ausgegeben werden. Um Fehlfunktionen aufgrund dieser Gefahr auszuschließen, werden beim Steuergerät gemäß Anspruch 5 die an den Steuerausgängen anliegenden Signale von mindestens einem der Rechner überprüft, und es wird eine Sicherheits-Steuerung vorgenommen, wenn festgestellt wird, daß die Werte der überprüften Signale nicht mit den erwarteten Werten übereinstimmen. Statt der an den Steuerausgängen anliegenden Signale können auch die Ausgangssignale der Steuerstufen überprüft werden, die von den Signalen der Steuerausgänge angesteuert werden, was Gegenstand von Anspruch 6 ist.

Die Funktionen zum Überwachen der beiden Rechner sowie die Funktionen zum Überprüfen der Korrektheit von Ausgangssignalen können einzeln oder gemeinsam angewendet werden. Von besonderem Vorteil ist es, alle Maßnahmen, die zum Erhöhen der Sicherheit beitragen, gemeinsam anzuwenden.

Zeichnung

Fig. 1 Blockschaltbild eines elektronischen Steuergerätes, das so ausgebildet ist, daß Ausgangssignale von einem Nebenrechner nur dann auf Steuerausgänge gegeben werden können, wenn ein dem Nebenrechner zugeordneter Watchdog ordnungsgemäßes Arbeiten des Nebenrechners anzeigt;

Fig. 2 Blockschaltbild eines elektronischen Steuergerätes, das so ausgebildet ist, daß Ausgangssignale von einem Nebenrechner nur dann auf einen Steuerausgang gegeben werden können, wenn ein dem Nebenrechner zugeordneter Watchdog ordnungsgemäßes Arbeiten des Nebenrechners anzeigt und gleichzeitig ein einem Hauptrechner zugeordneter Watchdog den Ausfall des Hauptrechners anzeigt;

Fig. 3 Blockschaltbild eines elektronischen Steuergerätes, das so ausgebildet ist, daß Ausgangssignale von einem Nebenrechner nur dann an einen Steuerausgang gegeben werden, wenn ein dem Nebenrechner zugeordneter Watchdog ordnungsgemäßen Betrieb des Nebenrechners anzeigt und entweder ein einem Hauptrechner zugeordneter Watchdog den Ausfall des Hauptrechners anzeigt oder wenn der Hauptrechner jeweils dasselbe Ausgangssignal abgibt wie der Nebenrechner; und

Fig. 4 Blockschaltbild eines elektronischen Steuergerätes, das Ausgangssignale überwacht, und das ein Sicherheitspotential auf einen Steuerausgang gibt, wenn festgestellt wird, daß die ermittelten Ausgangssignale nicht mit erwarteten übereinstimmen.

Beschreibung von Ausführungsbeispielen

Die Steuergeräte gemäß allen **Fig. 1 – 4** weisen einen Hauptrechner **10** mit zugehörigem ersten Watchdog **11**, einen Nebenrechner **12** mit zugehörigem zweiten Watchdog **13** und ein Signalausgabemittel **14** auf, das jeweils unterschiedliche Funktionsgruppen enthält. Das Signalausgabemittel **14** ist durch eine strichpunktierte Linie angedeutet. Von jedem der Steuergeräte wird mindestens ein Bauteil einer Brennkraftmaschine angesteuert. Bei **Fig. 1** sind es zwei Bauteile **15.1** und **15.2**. Jedes Bauteil erhält ein Steuersignal von mindestens einem Steuerausgang **16**. Das Steuergerät gemäß **Fig. 1** weist zwei Steuerausgänge **16.1** und **16.2** auf. Die Bauteile können Treiberstufen von Stellgliedern sein, es können aber auch Stellregler sein. Im ersten Fall stellt das ausgegebene Steuersignal ein Stellsignal dar, während es im zweiten Fall ein Sollwertsignal darstellt. An unterschiedlichen Steuerausgängen können unterschiedliche Arten von Steuersignalen ausgegeben werden. Es handelt sich jedoch immer um digitale Signale, also um Signale mit zwei Pegel. Jedes Bauteil **15** ist so ausgelegt, daß es dann, wenn ein vorgegebener Pegel dauernd auftritt, einen Zustand einstellt, der für einen solchen Betrieb der Brennkraftmaschine sorgt, der einen sicheren Betrieb des Fahrzeugs zur Folge hat, in dem die gesteuerte Brennkraftmaschine angeordnet ist. Das Potential des Pegels, bei dem der Sicherheitszustand eintritt, wird im folgenden Sicherheitspotential genannt. Es kann dies der niedrige oder der hohe Pegel des digitalen Ausgangssignales sein, je nachdem wie das angesteuerte Bauteil **15** ausgebildet ist.

Das Signalausgabemittel **14.1** beim Steuergerät gemäß **Fig. 1** weist ein Oder-Glied **17**, ein Und-Glied **18**, eine Umschalteinrichtung **19** und zwei Sperr-Und-Glieder **20.1** und **20.2** auf. Das Oder-Glied **17** empfängt die Signale vom ersten Watchdog **11** und vom zweiten Watchdog **13**. Sein Ausgangssignal ist ein Eingangssignal für die Sperr-Und-Glieder **20.1** und **20.2**. Das zweite Eingangssignal für das erste Sperr-Und-Glied **20.1** ist ein erstes Ausgangssignal HAS.1 vom Hauptrechner. Für das zweite Sperr-Und-Glied **20.2** ist das zweite Eingangssignal ein zweites Ausgangssignal HAS.2 vom Hauptrechner **10**. Das Ausgangssignal vom ersten Sperr-Und-Glied **20.1** gelangt an den ersten Steuerausgang **16.1**. Entsprechend wird das Ausgangssignal vom zweiten Sperr-Und-Glied **20.2** auf den zweiten Steuerausgang **16.2** geführt.

Die Sperr-Und-Glieder **20.1** und **20.2** erhalten die Ausgangssignale HAS.1 bzw. HAS.2 vom Hauptrechner **10** jedoch nur bei ordnungsgemäßem Betrieb dieses Rechners. Bei fehlerhaftem Betrieb schaltet die Umschalteinrichtung **19** um, wodurch die Sperr-Und-Glieder **20.1** und **20.2** Ausgangssignale NAS.1 bzw. NAS.2 vom Nebenrechner **12** erhalten. Das Umschalten erfolgt dann, wenn das Und-Glied **18** ein Ausgangssignal abgibt. Diese Und-Glied **18** erhält an seinem einen Eingang das Ausgangssignal vom zweiten Watchdog **13** und an seinem anderen Eingang ein Übernahmesignal US. Wenn beide Signale hohen Pegel einnehmen, erfolgt das Umschalten.

Die Verknüpfung der genannten Funktionsteile führt zum folgenden Ablauf.

Solange mindestens einer der beiden Watchdogs **11** und **13** ordnungsgemäßen Betrieb eines der beiden Rechner meldet, gibt das Oder-Glied **17** ein Signal hohen Pegels aus, das die beiden Sperr-Und-Glieder **20.1** und **20.2** auf Durchlaß schaltet. Diese stellen an ihrem Ausgang daher dasjenige Signal zur Verfügung, das am zweiten jeweiligen Eingang ansteht. Bei ordnungsgemäßem Betrieb ist dies das jeweilige Ausgangssignal HAS.1 bzw. HAS.2 vom Hauptrechner **10**. Fällt dieser jedoch aus, was vom Nebenrechner **12** dadurch festgestellt wird, daß über eine Datenaustauschleitung **21** fehlerhafte Signale oder keine Signale mehr empfangen werden, erfolgt das beschriebene Umschalten auf die Ausgangssignale NAS.1 bzw. NAS.2 vom Nebenrechner **12**. Dadurch, daß das Und-Glied **18** in der genannten Beschaltung vorhanden ist, ist sichergestellt, daß der Nebenrechner **12** ein Umschalten mit Hilfe des Über-

nahmesignales US nur dann vornehmen kann, wenn gleichzeitig der ihm zugeordnete zweite Watchdog 13 ordnungsgemäßen Betrieb des Nebenrechners 12 meldet. Bei bisher bekannten Steuergeräten war es möglich, daß der Nebenrechner aufgrund fehlerhaften Betriebs annahm, der Hauptrechner sei nicht in Ordnung, woraufhin er auf sein eigenes fehlerhaftes Ausgangssignal umschaltete. Dieser Mangel ist beim Steuergerät gemäß Fig. 1 weitgehend behoben.

Noch weitergehend läßt sich der eben genannte Mangel vermeiden, wenn ein Prinzip angewandt wird, wie es nun mit Hilfe des Steuergerätes gemäß Fig. 2 erläutert wird. Gemäß diesem Prinzip wird nämlich das Ausgeben des Signales vom Nebenrechner nicht nur dann verhindert, wenn dessen Watchdog den Ausfall des Nebenrechners anzeigt, sondern das Ausgeben wird auch dann verhindert, wenn der Nebenrechner 12 anzeigt, der Hauptrechner 10 sei ausgefallen, der dem Hauptrechner zugeordnete erste Watchdog 11 jedoch ordnungsgemäßen Betrieb des Hauptrechners 10 meldet.

Um das eben genannte Prinzip zu realisieren, ist im Signalausgabemittel 14.2 im Steuergerät gemäß Fig. 2 zusätzlich zu den Funktionsgruppen, die das Signalausgabemittel 14.1 gemäß Fig. 1 aufweist, noch ein zweites Und-Glied 22 vorhanden. Diesem, und nur diesem, werden die Ausgangssignale vom Oder-Glied 17 und vom Und-Glied 18 zugeführt, letzteres in negierter Form. Die Eingangssignale für das Oder-Glied 17 und das Und-Glied 18 sind die ausgehend von Fig. 1 beschriebenen Signale.

Der Einfachheit halber ist in Fig. 2, wie auch in den Fig. 3 und 4, nur jeweils ein Steuerausgang 16 mit angesteuertem Bauteil 15 dargestellt. Entsprechend gibt der Hauptrechner 10 nur ein einziges Ausgangssignal HAS und der Nebenrechner 12 nur ein einziges Ausgangssignal NAS aus. Es würde jedoch am Prinzip der Steuergeräte nichts ändern, wenn jeder der Rechner mehrere Ausgangssignale für mehrere Steuerausgänge ausgeben würde.

Der eben genannte Steuerausgang 16 erhält das Ausgangssignal vom Sperr-Und-Glied 20. Letzterem werden zwei Eingangssignale zugeführt, und zwar das Ausgangssignal vom zweiten Und-Glied 22 und das Ausgangssignal von der Umschalteinrichtung 19. Diese Umschalteinrichtung 19 wird bei der Variante gemäß Fig. 2 nicht mehr mit Hilfe eines Übernahmesignales US vom Nebenrechner 12 umgeschaltet, sondern mit Hilfe des Ausgangssignales vom ersten Watchdog 11. Sobald dieses Signal auf niedrigen Pegel fällt, schaltet die Umschalteinrichtung 19 vom Ausgangssignal HAS vom Hauptrechner 10 auf das Ausgangssignal NAS vom Nebenrechner 12 um.

Die eben beschriebene Ansteuerung der Umschalteinrichtung 19 gewährleistet, daß das Ausgangssignal NAS vom Nebenrechner 12 nicht auf den Steuerausgang 16 gelangen kann, solange der erste Watchdog 11 ordnungsgemäßen Betrieb des Hauptrechners 10 meldet. Stellt jedoch der Nebenrechner 12 gleichzeitig fehlerhaften Betrieb des Hauptrechners fest und gibt daher das Übernahmesignal US an das Und-Glied 18 aus, führt dies bei der oben genannten Schaltung dazu, daß das vom zweiten Und-Glied 22 an das Sperr-Und-Glied 20 ausgegebene Signal auf niedrigen Pegel fällt, weswegen das Sperr-Und-Glied 20 ein Dauersignal mit niedrigem Pegel auf den Steuerausgang 16 gibt. Dies wird erreicht, indem das Umschaltsignal US mit dem Watchdogsignal 13 im UND-Glied 18 verknüpft und invertiert auf den zweiten Eingang des zweiten UND-Gliedes geführt wird.

Bei der Schaltung gemäß Fig. 2 sperrt das Sperr-Und-Glied 20 also dann, wenn entweder die Signale von den beiden Watchdogs 11 und 13 ausfallen (niedriger Pegel am einen Eingang des zweiten Und-Gliedes 22) oder wenn der Nebenrechner 12 das Übernahmesignal US ausgibt und sein Watchdog 13 ordnungsgemäßen Betrieb des Hauptrechners 12 meldet (niedriger Pegel am anderen Eingang des zweiten UND-Gliedes 22). Auf das Ausgangssignal NAS vom Nebenrechner 12 wird nur dann umgeschaltet, wenn der erste Watchdog 11 den Ausfall des Hauptrechners 10 meldet.

Das Steuergerät gemäß Fig. 3 ist eine Variante des Gerätes gemäß Fig. 2, und zwar dahingehend, daß in demjenigen Fall, in dem der Nebenrechner 12 Ausfall, der erste Watchdog 11 jedoch ordnungsgemäßen Betrieb des Hauptrechners 10 meldet, nicht grundsätzlich dauernd das Sicherheitspotential an den Steuerausgang gegeben wird, sondern daß dann noch mit digitalen Signalen gesteuert wird, wenn die Ausgangssignale HAS vom Hauptrechner 10 und NAS vom Nebenrechner 12 übereinstimmen. Weiterhin ist das Ausführungsbeispiel dahingehend gegenüber dem von Fig. 2 variiert, daß keine Umschalteinrichtung 19 mehr vorhanden ist, sondern daß durch mehrere logische Funktionen gewährleistet wird, daß entweder das Ausgangssignal HAS vom Hauptrechner 10 oder das Ausgangssignal NAS vom Nebenrechner 12 auf den Steuerausgang 16 gelangt, oder beide Signale dorthin gelangen, nämlich unter der im vorigen Absatz genannten Bedingung.

Das Signalausgabemittel 14.3 im Steuergerät gemäß Fig. 3 weist ein Haupt-Und-Glied 24.1, ein Neben-Und-Glied 24.2, ein Signal-Oder-Glied 25.1 und ein Sperr-Oder-Glied 25.2 auf. Letzteres erhält als Eingangssignale die Ausgangssignale von den Oder-Gliedern 25.1 und 25.2. Dem Signal-Oder-Glied 25.1 werden die Ausgangssignale von den beiden genannten Und-Gliedern 24.1 und 24.2 als Eingangssignale zugeführt. Das Sperr-Oder-Glied 25.2 erhält als Eingangssignale die Ausgangssignale von den beiden Watchdogs 11 und 13. Das Ausgangssignal vom ersten Watchdog 11 gelangt darüber hinaus als Eingangssignal an das Haupt-Und-Glied 24.1. Entsprechend wird dem Neben-Und-Glied 24.2 als ein Eingangssignal das Ausgangssignal vom zweiten Watchdog 13 zugeführt. Das zweite Eingangssignal für das Haupt-Und-Glied 24.1 ist das Ausgangssignal HAS vom Hauptrechner 10, während das zweite Eingangssignal für das Neben-Und-Glied 24.2 das Ausgangssignal NAS vom Nebenrechner 12 ist.

Die Funktion des so aufgebauten Steuergerätes sei hier nochmals kurz zusammengefaßt: Melden sowohl der erste Watchdog 11 wie auch der Nebenrechner 12 ordnungsgemäßen Betrieb des Hauptrechners 10, gelangt dessen Ausgangssignal HAS an den Steuerausgang 16. Melden sowohl der ersten Watchdog 11 wie auch der Nebenrechner 12 Ausfall des Hauptrechners 10, gelangt das Ausgangssignal NAS vom Nebenrechner 12 an den Steuerausgang 16. Melden beiden Watchdogs 11 und 13 den Ausfall der zugehörigen Rechner 10 bzw. 12, liegt dauernd das Sicherheitspotential am Steuerausgang 16. Stellt schließlich der Nebenrechner 12 fehlerhaften Betrieb des Hauptrechners 10 fest, meldet jedoch der Watchdog 11 ordnungsgemäßen Betrieb des Hauptrechners 10, gelangt nur dann ein digitales Ausgangssignal an den Steuerausgang 16, wenn die Ausgangssignale HAS und NAS der beiden Rechner 10 und 12 übereinstimmen. Andernfalls liegt das Sicherheitspotential an.

Aus der vorstehenden Beschreibung ist ersichtlich, daß es für die erwünschte Betriebssicherheit darauf ankommt, daß die Watchdogs 11 und 13 ordnungsgemäß arbeiten. Um deren einwandfreie Funktion zu überprüfen, ist das Steuergerät in der Variante gemäß Fig. 4 so ausgestaltet, daß das Ausgangssignal vom ersten Watchdog 11 in den Hauptrechner 10 und das Ausgangssignal vom zweiten Watchdog 13 in den Nebenrechner 12 rückgeführt ist. In einem Prüfprogramm läßt der Hauptrechner 10 ein Triggersignal für den ersten Watchdog 11 ausfallen und überprüft, ob dann dessen Ausgangssignal auf niedrigen Pegel fällt. Ist dies nicht der Fall, zeigt dies fehlerhaften Betrieb des ersten Watchdogs 11 an, woraufhin der Hauptrechner 10 ein Notlaufsignal NLS.H an das Signalausgabemittel 14 ausgibt. Der Aufbau dieses Signalausgabemittels 14 ist in Fig. 4 nicht dargestellt. Es arbeitet vorzugsweise nach einem der anhand der Fig. 1–3 erläuterten Prinzipien. Auf das Notlaufsignal NLS.H hin, gibt das Signalausgabemittel 14 entweder das Sicherheitspotential an den Steuerausgang 16 oder es gibt ein solches digitales Signal aus, das zu einem stark eingeschränkten Fahrbetrieb führt. Dadurch wird der Fahrzeugführer veranlaßt, eine Werkstatt aufzusuchen, um das Steuergerät reparieren zu lassen.

Entsprechend wie der Hauptrechner 10 den ersten Watchdog 11 überprüft und bei Ausfall desselben ein Notlaufsignal NLS.H ausgibt, überprüft der Nebenrechner 12 den zweiten Watchdog 13 und gibt im Fehlerfall ein Notlaufsignal NLS.N aus.

Die eben genannte Überprüfung kann auch dann stattfinden, wenn keine zwei gesonderten Watchdogs vorhanden sind, sondern beide Rechner einen gemeinsamen Watchdog triggern. Der Hauptrechner 10 meldet dann dem Nebenrechner 12 über die Datenaustauschleitung 21, daß die Triggersignale ausgesetzt werden sollen. Dann überprüft einer der Rechner, ob das Ausgangssignal vom Watchdog abfällt. Ist dies der Fall, werden Notlaufmaßnahmen ergriffen.

Aus der vorstehenden Beschreibung ist ersichtlich, daß die verschiedenen Ausführungsformen der Signalausgabemittel alle dazu dienen, sicheren Betrieb einzustellen, wenn einer der Rechner ausfällt. Diesem Bestreben kann jedoch dann der Erfolg versagt sein, wenn das Signalausgabemittel selbst fehlerhaft arbeitet, oder wenn das angesteuerte Bauteil 15 das empfangene Signal falsch verarbeitet. Um auch in bezug auf derartige Fehler die Betriebssicherheit zu erhöhen, ist das Steuergerät gemäß Fig. 4 so ausgebildet, daß das Ausgangssignal vom Steuerausgang 16 sowohl auf den Hauptrechner 10 wie auf den Nebenrechner 12 rückgeführt ist. Jeder der Rechner kann dann überprüfen, ob das am Steuerausgang 16 auftretende Signal mit dem erwarteten Signal übereinstimmt.Entsprechend kann das Ausgangssignal vom Bauteil 15 auf die beiden Rechner rückgeführt und mit einem erwarteten Signal verglichen werden. Wenn sich bei einem der Vergleiche ein Fehler ergibt, wird ein Sperrsignal SPS.H oder ein Sperrsignal SPS.N vom Hauptrechner 10 bzw. vom Nebenrechner 12 ausgegeben. Diese Signale gelangen auf einen dem Bauteil 15 nachgeschalteten Sicherheitsschalter 26, der Massepotential oder ein anderes für den jeweiligen Anwendungsfall geeignetes Sicherheitspotential auf die Ausgangsleitung legt. Alternativ zum nachgeschalteten Sicherheitsschalter 26 kann der sichere Zustand auch durch einen in Fig. 4 nicht dargestellten, parallel zum Ausgang 16 mit Bauteil 15 arbeitenden zweiten Eingriff über einen weiteren Ausgang erfolgen, wie z. B. in Fig. 1 dargestellt.

Die anhand von Fig. 4 erläuterten Sicherungsmaßnahmen werden vorteilhafterweise gemeinsam eingesetzt, können jedoch auch einzeln verwendet werden. Von ganz besonderem Vorteil ist es, die anhand von Fig. 4 erläuterten Maßnahmen mit solchen zusammen einzusetzen, wie sie anhand von Fig. 2 oder von Fig. 3 beschrieben wurden.

Patentansprüche

1. Elektronisches Steuergerät für eine Brennkraftmaschine, mit
   - einem Hauptrechner (10),
   - einem Nebenrechner (12), der den Hauptrechner überwacht und bei Ausfall desselben Notfunktionen ausübt,
   - einer Watchdog-Schaltung (11, 13) für die Rechner, und
   - einem Signalausgabemittel (14; 14.1; 14.2; 14.3) zum Ausgeben von Signalen mit zwei Pegeln auf mindestens einen Steuerausgang (16; 16.1; 16.2), wobei einer der Pegel ein Sicherheitspotential aufweist, das bei dauerndem Vorhandensein für einen Sicherheits-Betriebszustand der Brennkraftmaschine sorgt,

dadurch gekennzeichnet, daß
   - ein erster Watchdog (11) zum Überwachen der Funktionen des Hauptrechners (10) vorhanden ist,
   - ein zweiter Watchdog (13) zum Überwachen der Funktion des Nebenrechners (12) vorhanden ist, und
   - das Signalausgabemittel (14.1) so ausgebildet ist, daß es
   - die Ausgangssignale vom Nebenrechner an den jeweils zugehörigen Steuerausgang (16.1, 16.2) gibt, wenn mindestens die Bedingungen erfüllt sind, daß der Nebenrechner ein Übernahmesignal ausgibt und gleichzeitig der zweite Watchdog meldet, daß der Nebenrechner ordnungsgemäß arbeitet,
   - aber grundsätzlich das Sicherheitspotential an jeden Steuerausgang gibt, wenn beide Watchdogs den Ausfall der überwachten Rechner melden.

2. Elektronisches Steuergerät nach Anspruch 1, dadurch gekennzeichnet, daß
   - das Signalausgabemittel (14.2) so weitergebildet ist, daß es
   - die Ausgangssignale vom Nebenrechner (12) nur dann an den jeweils zugehörigen Steuerausgang (16) gibt, wenn die Bedingung erfüllt ist, daß der erste Watchdog (11) den Ausfall des Hauptrechners (10) meldet, und
   - das Sicherheitspotential auch dann an jeden Steuerausgang gibt, wenn beide Watchdogs (11, 13) ordnungsgemäßen Betrieb der Rechner melden, aber der Nebenrechner fehlerhaften Betrieb des Hauptrechners meldet.

3. Elektronisches Steuergerät gemäß dem Oberbegriff von Anspruch 1, dadurch gekennzeichnet, daß
   - ein erster Watchdog (11) zum Überwachen der Funktion des Hauptrechners (10) vorhanden ist,
   - ein zweiter Watchdog (13) zum Überwa-

chen der Funktion des Nebenrechners (12) vorhanden ist, und

– das Signalausgabemittel (14.3) so ausgebildet ist, daß es

– die Ausgangssignale vom Nebenrechner dann an den jeweils zugehörigen Steuerausgang (16) gibt, wenn der zweite Watchdog ordnungsgemäßen Betrieb des Nebenrechners meldet und dabei der erste Watchdog den Ausfall des Hauptrechners meldet, aber auch dann, wenn beide Watchdogs ordnungsgemäßen Betrieb der Rechner melden, der Nebenrechner jedoch fehlerhaften Betrieb des Hauptrechners meldet, aber die Ausgangssignale der beiden Rechner für den Steuerausgang übereinstimmen,

– aber grundsätzlich das Sicherheitspotential an jeden Steuerausgang gibt, wenn beide Watchdogs den Ausfall der überwachten Rechner melden.

4. Elektronisches Steuergerät nach einem der vorstehenden Ansprüche, aber auch nach dem Oberbegriff von Anspruch 1, dadurch gekennzeichnet, daß

– die Rechner (10, 12) Überwachungssignale an die Watchdogschaltung (11, 13) geben und die Ausgangssignale der Watchdog-Schaltung nach dem Ausgeben der Überwachungssignale überprüfen, und

– der Hauptrechner (10) oder der Nebenrechner (12) dann das Sicherheitspotential ausgeben, wenn die Überprüfung ergibt, daß die zum jeweiligen Rechner gehörende Watchdog-Schaltung nicht ordnungsgemäß arbeitet.

5. Elektronisches Steuergerät nach einem der vorstehenden Ansprüche oder nach dem Oberbegriff von Anspruch 1, dadurch gekennzeichnet, daß

– die an den Steuerausgängen (16) anliegenden Signale von mindestens einem der Rechner (10, 12) überprüft werden, und

– eine Sicherheits-Steuerung vorgenommen wird, wenn festgestellt wird, daß die Werte der überprüften Signale nicht mit den erwarteten Werten übereinstimmen.

6. Elektronisches Steuergerät nach einem der vorstehenden Ansprüche oder nach dem Oberbegriff von Anspruch 1, dadurch gekennzeichnet, daß

– die Ausgangssignale angesteuerter Bauteile (15) von mindestens einem der Rechner (10, 12) überprüft werden, welche Bauteile von den Signalen am jeweils zugehörigen Steuerausgang (16) angesteuert werden, und

– eine Sicherheits-Steuerung vorgenommen wird, wenn festgestellt wird, daß die Werte der überprüften Signale nicht mit den erwarteten Werten übereinstimmen.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 39 26 377 A1
Int. Cl.5: F 02 D 41/22
Offenlegungstag: 7. Februar 1991

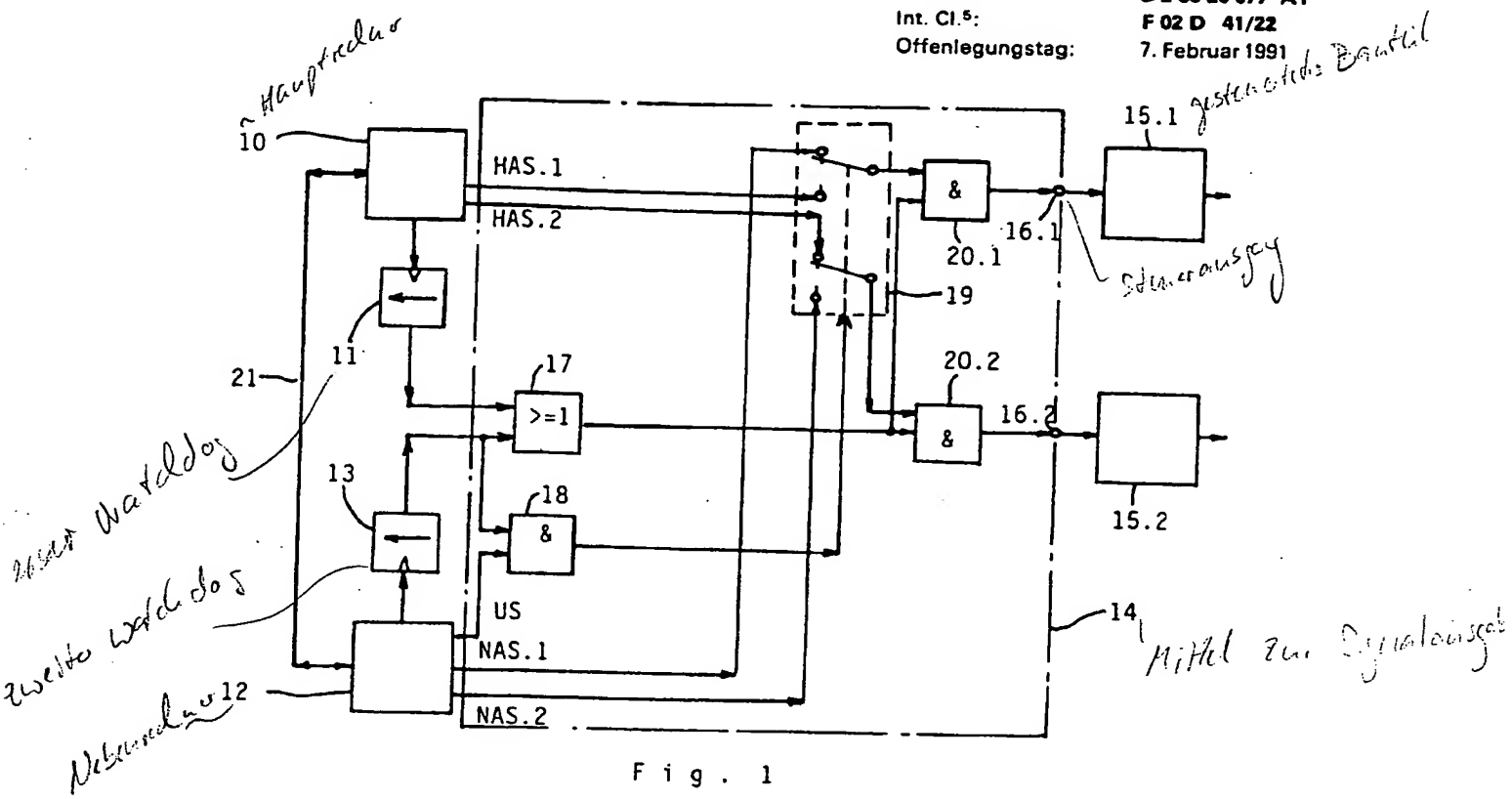


Fig. 1

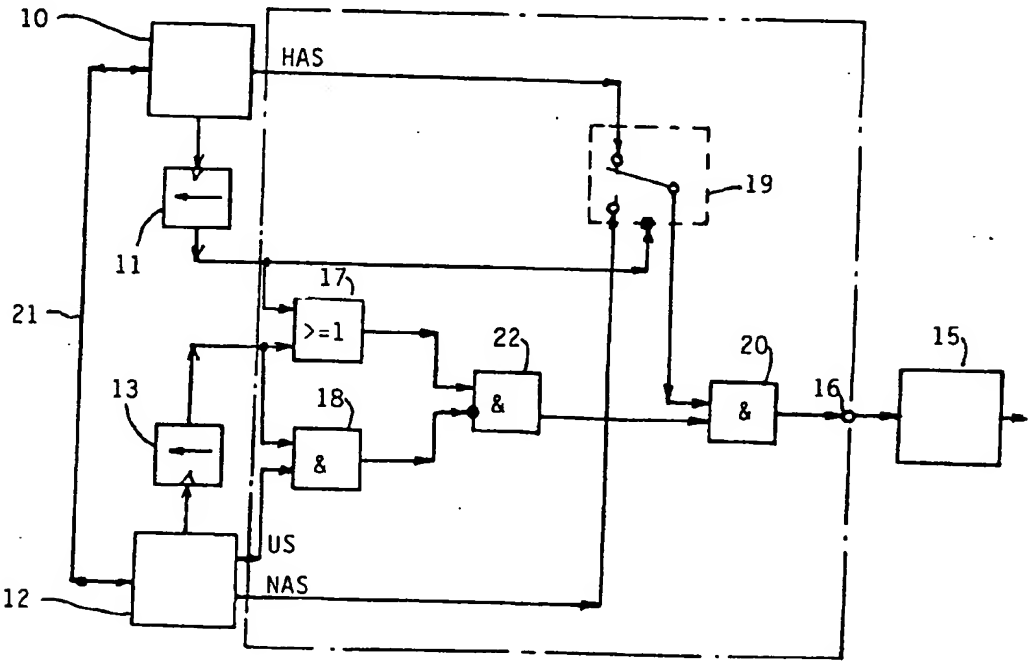


Fig. 2

Nummer: DE 39 26 377 A1
Int. Cl.[5]: F 02 D 41/22
Offenlegungstag: 7. Februar 1991

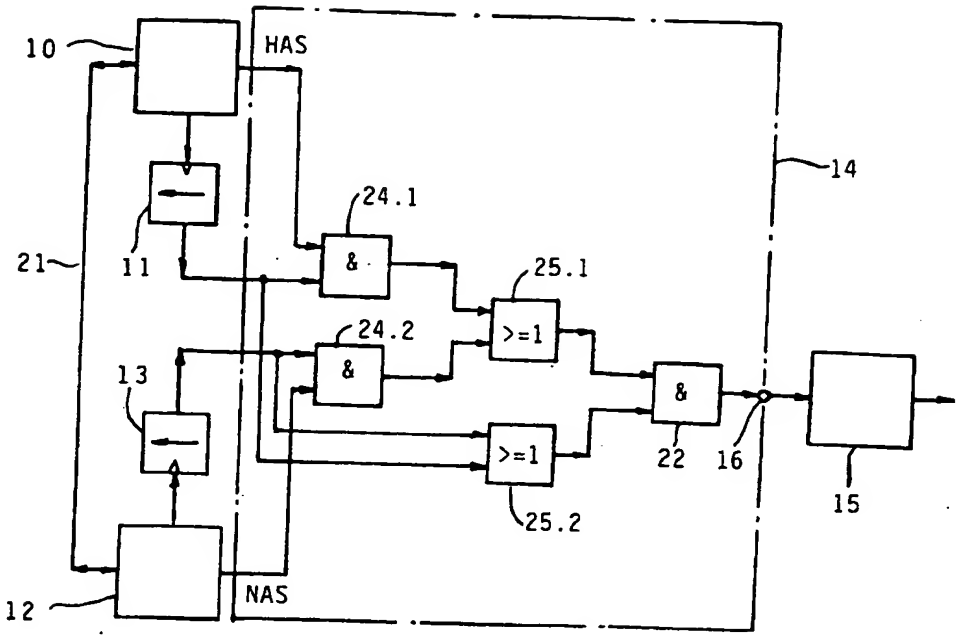


Fig. 3

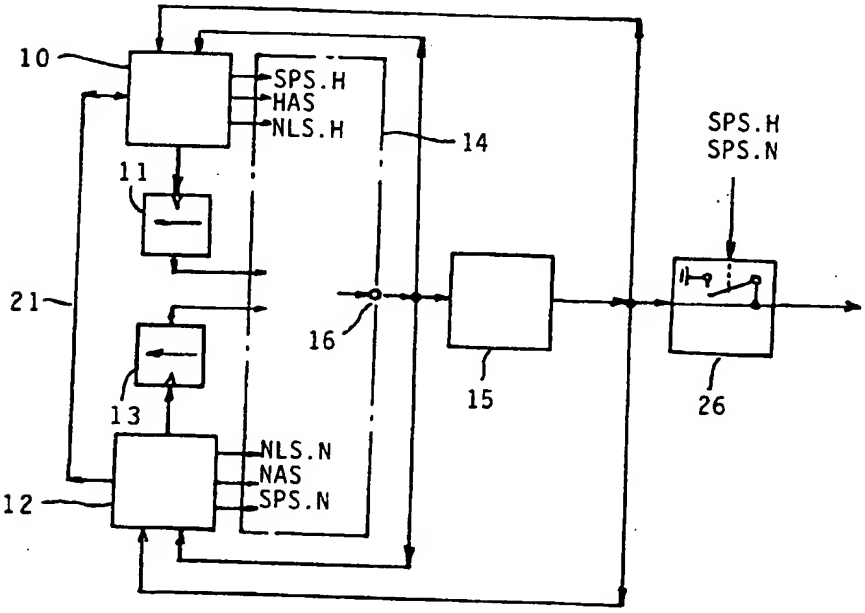


Fig. 4

AN: PAT 1991-04521[redacted]
TI: Two-watchdog electronic control equipment for IC engine provides self-checking of both computers and switches out faulty computer supplying two driver outputs
PN: **DE3926377**-A
PD: 07.02.1991
AB: Main (10) and standby (12) computers have their own watchdogs (11,13) and provide outputs to a control signal distributor (14) serving two drivers (15.1, 15.2) or position controllers from a change-over switch (19) and two blocking AND/gates (20.1, 20.2). One level of output represents a security potential setting the driver (15) into a security operational state. If both m computers (10,12) are found defective by their watchdogs (11,13) this potential appears at both outputs.; For e.g. diesel fuel injection pumps. Main and standby computer combination guarantees delivery of control signals with very high probability of their proper computation.
PA: (BOSC) BOSCH GMBH ROBERT;
IN: DANILIDIS G; FAHRBACH W; GRAF H; LOCHER J; ZIMMERMANN W; DANIILIDIS G;
FA: **DE3926377**-A 07.02.1991; **DE3926377**-C2 06.03.2003; JP11190251-A 13.07.1999; JP2983532-B2 29.11.1999;
CO: DE; JP;
IC: F02D-041/22; F02D-041/26; F02D-041/36; F02D-045/00;
MC: X22-A03A1; X22-A05;
DC: Q52; X22;
FN: 1991045218.gif
PR: DE3926377 04.08.1989;
FP: 07.02.1991
UP: 19.03.2003